10

MANAGING DFS, DISK QUOTAS, AND SOFTWARE INSTALLATION

After reading this chapter and completing the exercises you will be able to:

♦ Design, configure, and manage the Distributed File System (Dfs) on a network

♦ Publish a shared folder and a Distributed File System shared folder in the Active Directory

♦ Enable and configure disk quotas

♦ Install and manage application software

♦ Edit and configure the Windows 2000 Server Registry

♦ Set up and use the Microsoft License Manager

Implementing servers with shared folders on a network sometimes translates into a steep learning curve for users as they attempt to determine how to find folders and files that they need to use. The learning curve increases with the number of server names to remember and the number of shared folders to access. Naming servers for their function has been one way to help users learn which server contains which resource. The Microsoft Distributed File System (Dfs) makes it even easier for users, because multiple shared folders and files located on multiple servers can be set up so that they appear under one folder on one server. Using the Distributed File System is a simple way to enable users to be immediately productive on a server network without the learning curve. Another reason for using the Distributed File System is to enable Windows 2000 Server file-sharing capabilities to match the distributed model of computing in enterprise networks, in which data and applications are spread throughout several server locations. The popularity of client/server applications has made distributed computing options essential in a server operating system.

In the sections that follow, you discover not only how to set up the Distributed File System on a network, but how to plan the setup before you implement it. Another part of setting up shared network folders and the Distributed File System is to use **disk quotas** to help you plan disk capacity and to ensure that users do not prematurely consume all of the disk capacity. You also learn how to install software on a server and how to edit the server Registry, which contains a wealth of hardware and software configuration information. Last, you learn about managing software licensing by using the License Manager.

CONFIGURING AND USING THE DISTRIBUTED FILE SYSTEM

The **Distributed File System** (**Dfs**) enables you to simplify access to the shared folders on a network by setting up folders to appear as if they are accessed from only one place. If the network, for example, has eight Windows 2000 servers that make a variety of shared folders available to network users, Dfs can be set up so that users do not have to know which server offers which shared folder. All of the folders can be set up to appear as though they are on one server and under one broad folder structure. Dfs also makes managing folder access easier for server administrators. Dfs is configured using the Distributed File System tool in the Administrative Tools menu (click Start, point to Programs, and point to Administrative Tools) or the Distributed File System MMC snap-in.

If Dfs is used in a domain, then shared folder contents can be replicated to one or more DCs or member servers, which means that if the original server goes offline, its shared folders are still available to users through the replica servers. Also, from the server administrator's perspective, he or she can update software in a shared folder without having to make the folder temporarily inaccessible during the update. Dfs offers the following advantages:

- Shared folders can be set up so that they appear in one hierarchy of folders, enabling users to save time when searching for information.

- NTFS access permissions fully apply to Dfs on NTFS-formatted volumes.

- Fault tolerance is an option by replicating shared folders on multiple servers, resulting in uninterrupted access for users.

- Access to shared folders can be distributed across many servers, resulting in the ability to perform **load balancing**, so that one server does not experience more load than others.

- Access to resources for Web-based Internet and intranet sites is improved.

- Vital shared folders on multiple computers can be backed up from one set of master folders.

> **TIP** When you plan to use Dfs, strongly consider implementing it on a volume formatted with NTFS so that security capabilities such as access permissions, special permissions, and auditing can be used.

Besides enabling users to be more productive, Dfs also allows server administrators to be immediately more productive because Dfs reduces the number of calls to server administrators asking where to find a particular resource. Another advantage of Dfs in a domain is that folders can be replicated automatically or manually through Microsoft Replication Services (described later in this chapter). Shared folders in Dfs are copied to each designated replica computer, which yields two significant advantages: (1) important information is not lost when a disk drive on one server fails, and (2) users always have access to shared folders, even in the event of a disk failure.

In the pre-Dfs model of sharing, in Windows NT Server for instance, one or two servers might bear the brunt of most network activity because of heavy access to their shared folders. For example, consider a busy college network in which student registration information is housed in shared folders on one server. During registration that server is destined to experience extremely heavy access, delaying registration and causing students to wait in lines or be placed on hold when registering by telephone or through the Internet. If Dfs is implemented, the critical registration folders are replicated to multiple servers, causing access to be equally distributed among those servers. The result is faster registration and fewer headaches for students and the registrar's office. The same load-balancing features can be used to improve Web access by distributing the load among many servers. This is especially important, for example, to companies that rely on e-commerce for much of their business, because the companies can handle higher volumes of customer traffic and, at the same time, their customers are happier because they do not have to wait to transact business.

10

> **TIP** In a mixed-mode domain that has a combination of Windows 2000 and Windows NT 4.0 servers, Dfs can be fully implemented on the Windows NT 4.0 servers as long as Service Pack 3 or above is installed.

Dfs Models

There are two models for implementing Dfs: standalone and domain-based. The standalone Dfs model offers more limited capabilities than the domain-based model. In the standalone model there is no Active Directory implementation to help manage the shared folders, and this model provides only a single or flat level share, which means that the main Dfs shared folder does not contain a hierarchy of other shared folders. Also, the standalone model does not have Dfs folders that are linked to other computers through a Dfs container that has a main root and a deep, multilevel hierarchical structure.

The domain-based model of Dfs has more features than the standalone approach. Most importantly, the domain-based model takes full advantage of the Active Directory and is available only to servers and workstations that are members of a domain. The domain-based model enables a deep root-based hierarchical arrangement of shared folders that is published in the Active Directory. Dfs shared folders in the domain-based model are replicated for fault tolerance and load balancing, whereas the standalone Dfs model does not implement these features.

Dfs Topology

The hierarchical structure of Dfs in the domain–based model is called the **Dfs topology**. There are three elements to the Dfs topology:

- The Dfs root
- The Dfs links
- Servers on which the Dfs shared folders are replicated as replica sets

A **Dfs root** is a main container in the Active Directory that holds links to shared folders that can be accessed from the root. The server that maintains the Dfs root is called the host server. When a network client views the shared folders in the Dfs root, all of the folders appear as though they were in one main folder on the Dfs root computer, even though the folders may actually reside on many different computers in the domain.

A **Dfs link** is a designated access path between the Dfs root and shared folders that are defined to the root. For example, a Dfs root might be set up to contain all shared research folders for a plant biology research group that has folders on four different servers. Those folders can be shared via links drawn from them to the Dfs root so that all of the folders appear as though they were available from one place through the published information in the Active Directory. Dfs links can also be made to another Dfs root on a different computer or to an entire shared volume on a server (see Figure 10-1).
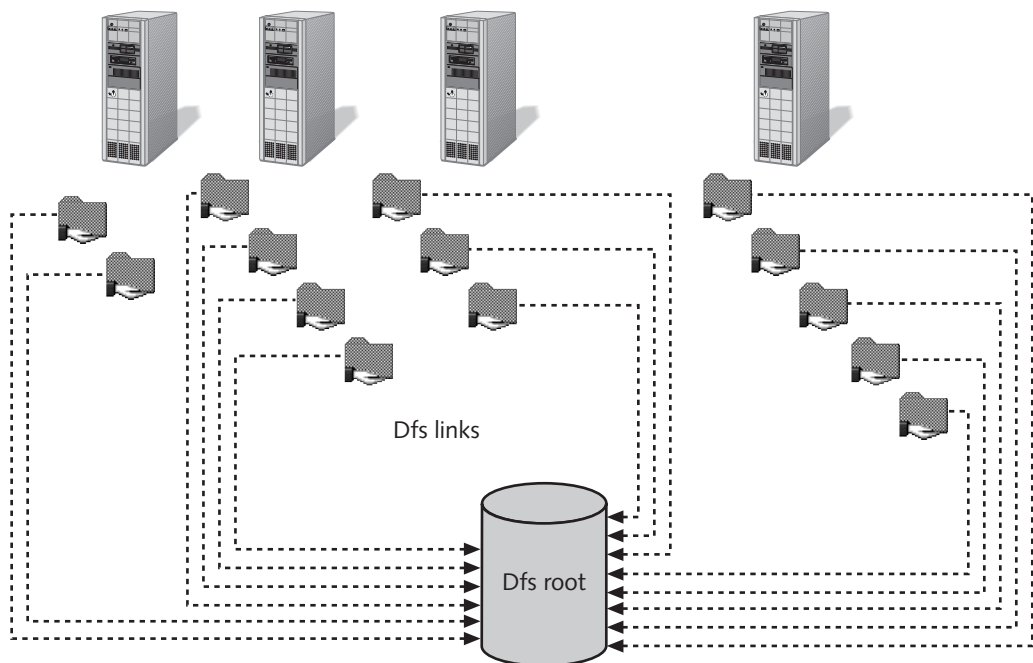
Figure 10-1   Dfs links in the Dfs root container

A **replica set** is a set of shared folders that is replicated or copied to one or more servers in a domain. In the plant biology example, the replica set would consist of all shared folders under the Dfs root that are designated to be replicated to other network servers. Part of this process establishes links to each server that participates in the replication. Another part of the process is to set up synchronization so that replication takes place among all servers at a specified interval, such as every 15 minutes.

Planning a Dfs Implementation

A Dfs implementation is most successful when it is well planned. There are several factors that Microsoft recommends you consider before installing and setting up Dfs:

- First, determine whether to use a standalone or domain-based model. On networks that deploy the Active Directory, the domain-based model provides the most options and enables you to manage the resulting network traffic. If you have a small network and have not deployed the Active Directory, then your only choice is to use the standalone model.

- Regardless of whether the standalone or domain-based model is used, place Dfs shared folders on disks that are formatted using NTFS, to ensure that there are strong security options.

- Consider using more than one Dfs root to reflect the particular needs of an organization. For example, in a college that has several divisions, such as arts and sciences, business, and engineering, there might be separate roots on different servers to reflect each division. Also there might be trees within a root for each department such as anthropology, art, biology, chemistry, English, physics, psychology, sociology, and so on, for the division of arts and sciences.

- Each time you manage Dfs through the MMC, save the console changes when you exit, so that they are available to you in your next management session.

- Set up a short cache timeout on folders with contents that change often.

- Determine the impact that Dfs will have on network traffic. If you determine there will be high-volume use of Dfs folders, consider using the domain-based model so that you can provide load balancing. Keep in mind that when you use load balancing in the domain-based model, Dfs is able to work with a DNS server to connect each user to the closest server providing Dfs services.

- When designing a domain-based model, create the first Dfs root and links to that root before creating additional Dfs roots.

- In the domain-based model, develop a synchronization schedule that will take into account the existing network traffic along different routes (segments) on which synchronization will occur. For example, synchronize more frequently on routes that have high-speed links, such as 100 Mbps, and less frequently on lower-speed routes that operate at 10 Mbps.

- Review all Dfs shared folders on a regular basis so that you can purge folders that are no longer in use.

10

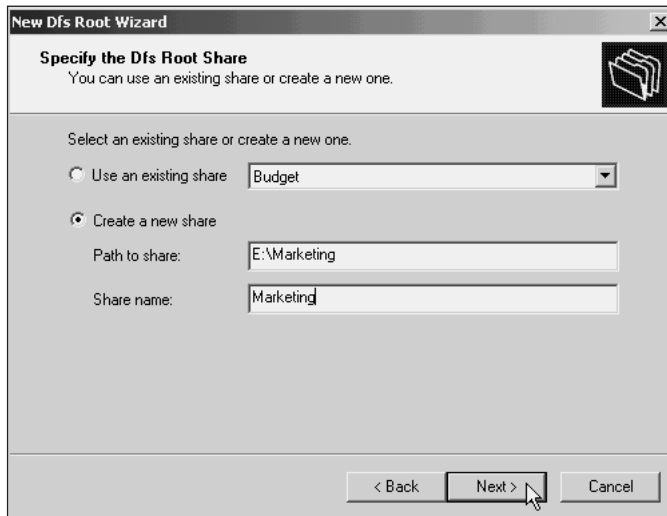## Configuring the Standalone Dfs Model

The Distributed File System management tool can be accessed in two ways. One is to set it up as an MMC snap-in, and the other is to open it by clicking Start, pointing to Programs, pointing to Administrative Tools, and clicking Distributed File System. After the Distributed File System management tool is started:

1. Click the Action menu and click New Dfs Root to start the New Dfs Root Wizard.

2. Click Next.

3. Click Create a standalone Dfs root, and click Next (see Figure 10-2).


Figure 10-2   Specifying the standalone model

4. Enter the name of the server that will host the Dfs root and click Next.

5. Click Use an existing share, if you want to implement Dfs to use a shared directory that is already created on the server. The text box provides a list of all of the possible selections. Otherwise, click Create a new share to set up Dfs from a shared directory that does not presently exist. If you are creating a new share, then provide the path to the share and the name of the share (see Figure 10-3). Click Next.

6. If creating a new share, click Yes to create the new folder, if it does not already exist.

7. The wizard assigns a unique name for the root folder, which is the same as the share name specified in Figure 10-3. Enter a comment to describe the share, and then click Next.

8. Review the information that has been entered, and click Finish; or click Back to go back and change information that is already entered.

Figure 10-3   Creating a new Dfs share

After the standalone Dfs shared root folder is created, it is displayed in the Distributed File System console window, as shown in Figure 10-4. If you are using the MMC, make sure that you save the changes and provide a name for the console, so that you can easily view the Dfs shared folder the next time that you open the console. If the Dfs shared folder is not displayed the next time you access the MMC snap-in, because it was not saved, install the Distributed File System snap-in again. After the snap-in is installed, click Distributed File System under the Console Root, click the Action menu, click Display an Existing Dfs root, enter the server name and Dfs shared folder name, and click OK.
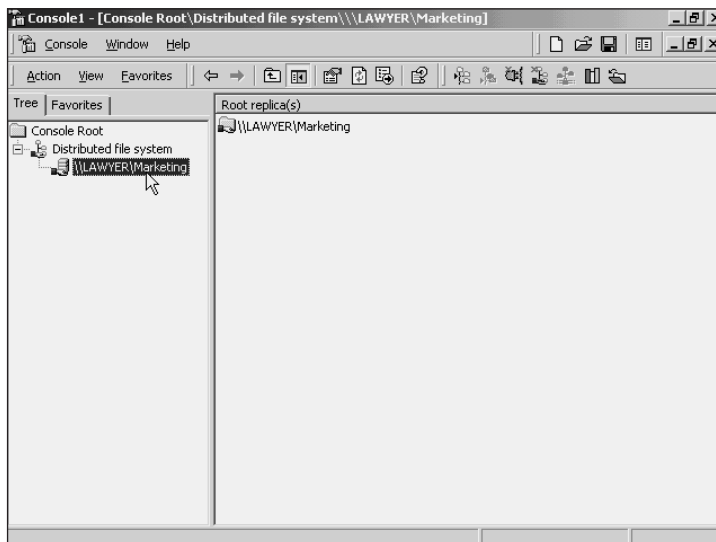
**Figure 10-4**   Viewing a new Dfs shared folder in the MMC console

> **TIP** If you attempt to create a standalone root on a server, and see the error message, "This server already hosts a Dfs root," this means that you cannot create an additional Dfs root on that server because one already exists, and a host server can have only one.

Configuring the Domain-based Dfs Model

Installing a domain-based Dfs root is similar to installing a standalone Dfs root, but there are some differences, such as specifying the domain in which the root resides. Use the following steps to set up a domain-based Dfs root:

1. Open the Distributed File System management tool as an MMC snap-in or from the Administrative Tools menu. If the Distributed File System snap-in is used, click Distributed file system under the Console Root.

2. Click the Action menu and click New Dfs root, or click the Create a new Dfs root icon on the button bar.

3. Click Next after the New Dfs Root Wizard starts.

4. Click Create a domain Dfs root.

5. Enter the name of the domain in which the root will reside (see Figure 10-5). Click Next.
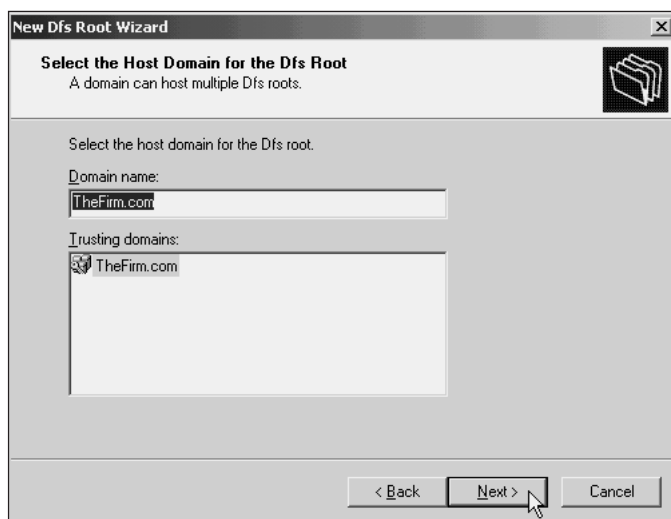
Figure 10-5 Entering the domain name

6. Enter the server name, or use the browse button to find the server and then click Next. The server name will be identified with the domain in which it resides.

7. Click the appropriate radio button to use an existing shared folder, or select the option to create a new shared folder. If you create a new shared folder, also provide

the path to the share and the share name (refer to Figure 10-3). Click Next. If you select Create a new share, click Yes to create the new folder for the share.

8. Enter the Dfs root name, or use the default already provided, which is the share name that you provided in the last step. Also, enter a comment to describe the root, and then click Next.

9. Examine the summary of information that you specified, and click Finish; or click Back to reenter information.

Try Hands-on Project 10-1 to practice setting up a new Dfs root.

Managing a Domain-based Dfs Root System

After the Dfs root system is set up, there are several tasks involved in managing the root, which can include:

- Deleting a Dfs root
- Adding and removing a Dfs link
- Adding root and link replica sets
- Configuring security
- Checking the status of a root or link

Each of these tasks is described in the following sections.

Deleting a Dfs Root

After a Dfs root is created, it is possible to delete it—when you want to configure it differently, for example. To delete a Dfs root:

1. Provide users with a warning that the root will be deleted, to make sure that no one is accessing the root when you delete it.

2. Open the Distributed File System management tool via the MMC or from the Administrative Tools menu.

3. Right-click the root that you want to delete under Distributed file system in the tree.

4. Click Delete Dfs Root.

5. Click Yes.

CAUTION

Keep in mind that when a domain-based Dfs root is deleted, so are the shared folder links to that root.

(You can practice deleting a Dfs root in Hands-on Project 10-3.)

Adding and Removing a Dfs Link

A link to a Dfs root can be established to a shared folder on the same computer as the root or to another computer that is a member of the domain. For example, there might be three servers that contain spreadsheets that should be placed under the Dfs root for easy access. To set up a link, follow these steps:

1. Open the Distributed File System management tool and right-click the root under the tree in the left pane.

2. Click New Dfs Link.

3. Enter a name that users will see (as a shared folder under the Dfs root folder) for the link (see Figure 10-6). Use the Browse button to find the computer and shared folder that you want to link to the Dfs root. Provide a comment to describe the link.
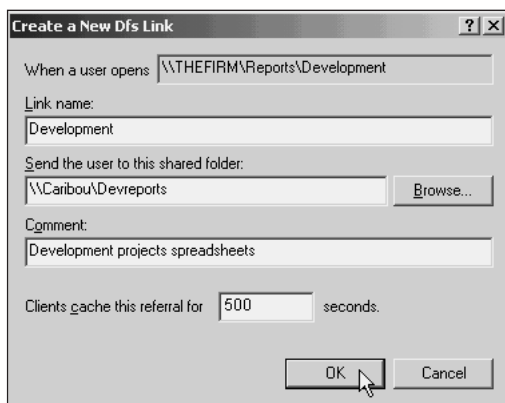
Figure 10-6   Creating a Dfs link

4. Establish the cache timeout (described in the following paragraph) in seconds for the link.

5. Click OK.

When you create a link, the first link automatically becomes the **master folder** for replication, which is the folder that contains the master copy replicated to the other links. It is listed in the right pane of the Distributed File System tool under the Replica(s) column. Also, the security, such as access permissions and auditing, that is already set up for the shared folder that becomes a link to a Dfs root is retained after the link is established. The **cache timeout** is the amount of time that a shared folder is retained in the client operating system's cache for fast access. A typical implementation for the timeout value is 300 seconds. Increase this amount by several hundred seconds, if you anticipate that the contents in the link will be changed often, and decrease the amount to 100 or 200 seconds if the contents will be changed less frequently.

> TIP   The cache timeout can be adjusted after a Dfs link is created by right-clicking the link and resetting the cache timeout in the General tab.

A link is removed from the Dfs root by using the following steps:

1. Right-click the link in the left pane.
2. Click Remove Dfs Link.
3. Click Yes.

Hands-on Project 10-2 enables you to practice creating and deleting Dfs links.

Adding Dfs Root and Link Replicas

An entire Dfs root or specific Dfs links in a root can be replicated on servers other than the one that contains the master folder. The replication capability is what enables you to provide fault tolerance and to create load balancing. On a network in which there are multiple servers, replication can prove to be a vital service to provide uninterrupted access for users, in case the computer with the master folder is inaccessible. Load balancing also is vital as a way to provide users with faster service and better network performance by enabling users to access the nearest server containing the Dfs shared folders.

You can replicate the root and all of its links to shared folders to one or more computers other than the one that houses the original Dfs root and links. Any computer that contains a replica of the original root and links cannot already have any Dfs roots, because you can only create one root per computer. To create a replica of an entire root, first determine which domain controllers or member servers do not already contain a Dfs root. Next, right-click the Dfs root that you want to replicate using the Distributed File System management tool. Click New Root Replica, and use the New Dfs Root Wizard to provide the name of the server on which to place the replica, the path for the replica, and whether to manually or automatically synchronize the information between the master and the replica.

The replication is handled by the Windows 2000 File Replication service. If automatic synchronization is used, then the default synchronization interval is every 15 minutes. When manual synchronization is used instead of automatic, then new links must be manually built in each root replica by an administrator. Normally, you will set up to use automatic synchronization, but manual synchronization is an alternative if you do not want to fully replicate all links, for example. If you attempt to create a Dfs root replica on a server that already has a root, the New Dfs Root Wizard provides a message that one already exists on that computer. Also, if you try to create a Dfs root replica on a Windows NT 4.0 server, but receive an error message, check two possibilities: (1) Service Pack 3 or above is not installed on the Windows NT 4.0 server, or (2) you have previously converted the domain from mixed mode to native mode, and Windows NT 4.0 servers are no longer recognized as viable server members.

Depending on the domain and server Dfs architecture and planning, it may be desirable to replicate designated Dfs links. For example, you might set up link replication as a way to

10

load-balance access to specific folders on a busy network. Consider a business campus on which the accounting office is located several buildings away from the budget office. A Dfs link to shared accounting files might be replicated on servers that are located near the accounting department, while a link to shared budget files is replicated on a server located near the budget office. To set up replication of a designated link:

1. Right-click the Dfs link in the Distributed File System tool, and click New Replica.

2. Enter the computer name and shared folder on the computer to use for the replica, or use the browse button to locate the computer and shared folder in the domain. The computer name and shared folder are specified in UNC format.

3. Click Manual replication or Automatic replication, and then click OK (see Figure 10-7).
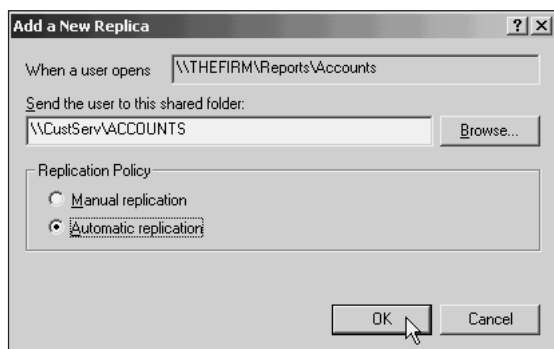
Figure 10-7   Adding a new replica for a Dfs link

4. If you selected Automatic replication in Step 3, set the replication policy, which enables you to change the master folder and to designate which replicas are enabled for automatic replication. Click OK.

5. The replica computer and folder path is added under the Replica(s) column in the Dfs tree for the designated link.

A Dfs root replica can be deleted by clicking the Dfs root, right-clicking the replica to be deleted under the Root replica(s) column, and then clicking Remove replica. Similarly, a replica of a Dfs link is deleted by clicking the Dfs link, right-clicking the link in the Replica(s) column, and clicking Remove replica.

After the first Dfs root or Dfs link replica is established, you can modify the replication pol-icy for either one by right-clicking the Dfs root or link and clicking Replication Policy. The Replication Policy dialog box (see Figure 10-8) is used to enable or disable replication to a specific server and to set the master folder. Also, the cache timeout can be set on a Dfs root or link by right-clicking it in the Distributed Files System management tool and clicking Properties. Use the "Clients cache this referral for _____ seconds" parameter to set the timeout value (Hands-on Project 10-2 enables to you practice setting the cache timeout).
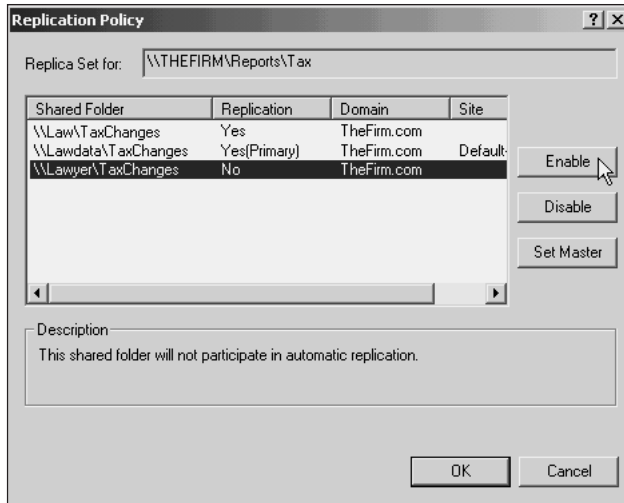
Figure 10-8   Configuring replication policy

Configuring the File Replication Service

Because automatic Dfs replication relies on the File Replication service, it is important to make sure that the service is started and that it is set to start automatically each time that the server is booted. The File Replication service is designed to synchronize the contents of folders between two or more Windows 2000 servers. The service consists of two broad functions within a single service. One function is to maintain information about each set of folders and associated servers to replicate, along with the process used to perform the replication. The second function is to establish connectivity between servers for the replication process.

When you configure Dfs replication, make sure that the File Replication service is configured. Click Start, point to Programs, point to Administrative Tools, and click Computer Management. Double-click Services and Applications in the left pane, and double-click Services in the right pane. Find the File Replication Service and make sure that the status is *Started* and that the Startup Type is *Automatic.* If you need to configure one or both of these settings, double-click File Replication service, set the Startup type box to Automatic, and click the Start button.

Configuring Security

The security on Dfs shared folders is inherited from the access and share permissions already established on those folders. Overall security for the Dfs root can be fine-tuned by applying permissions, auditing, and ownership parameters. The permissions to the contents of the Dfs root that can be allowed or denied to any user account, group, or computer are:

- *Full Control:* The ability to change permissions, take ownership, create, delete, modify, and manage Dfs shared folders and files; and the ability to delete trees and subtrees within the folder structure
- *Read:* The ability to list and read the contents of shared folders and files
- *Write:* The ability to modify the contents of shared folders and files

The security for a Dfs root is configured by right–clicking the root in the Distributed File System management tool, clicking Properties, and clicking the Security tab (if the Dfs root is located on an NTFS-formatted disk). The Security tab is nearly identical to the Security tab that is used for an ordinary folder. User accounts, groups, and computers are added by clicking the Add button and specifying the permissions (see Chapter 9).

Special permissions can be set up by clicking the Advanced button on the Security tab and then clicking View/Edit. The Advanced button on the Security tab also enables you to audit access to the Dfs root or to take ownership. Auditing works by monitoring successful and failed attempts to use any of the special permissions, such as successful attempts to list the root contents or failed attempts to delete the contents of the Dfs root. Auditing can be set by user account, group, and computer. Ownership of a Dfs root is taken via the Ownership tab.

Checking the Status of a Root or Link for Troubleshooting Connectivity

The most common problem associated with Dfs shared folders is that one or more Dfs links are inaccessible because a particular server is disconnected from the network or has failed. You can quickly check the status of a Dfs root, Dfs link, or replica by right-clicking it in the Replica(s) column of the Distributed File System management tool and then clicking Check Status. A Dfs root, link, or replica that is working and fully connected will have a green check mark in a white circle through its folder icon. One that is disconnected will have a white "x" in a red circle (see Figure 10-9) through its folder icon.
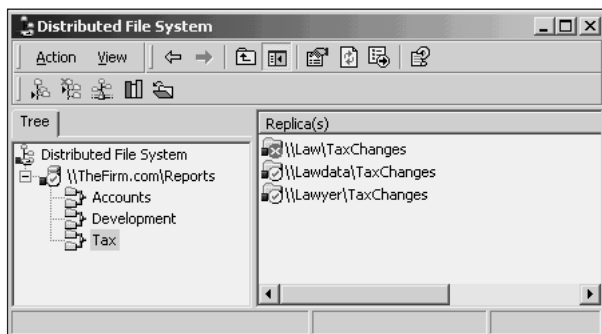
**Figure 10-9** Checking the status of replicas in a link

PUBLISHING A SHARED FOLDER

When you set up regular shared folders or Dfs root folders, you can publish them in the Active Directory. It is not mandatory to publish them, but that provides yet another way to make them easy for users to find and access.

To publish a shared folder or a Dfs root:

1. Open the Active Directory Users and Computers tool.

2. Right-click the domain.

3. Point to New and click Shared Folder.

4. Enter the name for the published folder that users will see in the Active Directory.

5. Enter the path to the shared folder or Dfs root (see Figure 10-10), and click OK.
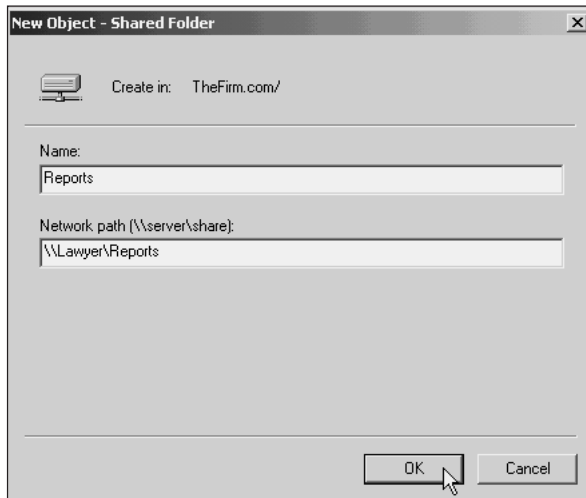
Figure 10-10   Publishing a shared folder

The domain objects displayed in the right pane for the domain in the Active Directory Users and Computers tool will now show a shared folder/drive icon. When you double-click the icon, you can enter a description of the shared folder or Dfs root, change the path (in case it is moved to another computer), and associate keywords that can be used to help identify its contents, so that when users search the Active Directory using those keywords, the published shared folder or Dfs root will be displayed. To associate keywords, double-click the folder, access the General tab, click the Keywords button, and enter the desired keywords for searches.

Windows 2000 Professional users can find the published folder by searching the Active Directory, using My Network Places, or the Start button, Search option (to search My Network Places). Windows 95, 98, and NT users also can employ the Directory Service Client (DSClient, see Chapter 8) software to search the Active Directory for the published folder.

CONFIGURING DISK QUOTAS

Another reason to set up shared folders and Dfs shared folders using NTFS-formatted volumes is to activate the ability to establish disk quotas. Using disk quotas has the following advantages:

- Prevents users from filling the disk capacity

- Encourages users to help manage disk space by deleting old files when they receive a warning that their quota limit is approaching

- Tracks disk capacity needs on a per-user basis for future planning

- Provides server administrators with information about when users are nearing or have reached their disk quotas

Disk quotas can be set on any local or shared volume. By simply enabling the disk quota feature on a volume, you can determine how much disk capacity is occupied by each user, without specifically setting quotas on those users. Another option is to set default quotas for all users, particularly on volumes that house user home folders. For example, many organizations establish a default quota of 10 to 100 MB per user on home folder volumes. The default quota prevents a few users from occupying disk space that is needed for all users. Disk quotas also can be established on a per-user basis, or special exceptions can be made for users who need additional space, such as a newspaper publishing group on a college campus that requires a large amount of space for text and graphics files.

> **TIP** Plan to establish disk quotas before offering shared and Dfs shared folders to network users. It is politically much easier to set quotas in the beginning than to set quotas after users have grown used to having no limits.

The general parameters that can be configured for disk quota management include:

- *Enable quota management:* Starts tracking disk quotas and sets up quota management

- *Deny disk space to users exceeding quota limit:* Prevents users from writing new information to disk after they have exceeded their quotas

- *Do not limit disk usage:* Tracks disk usage without establishing quotas on users, for example to gather statistics for disk-capacity planning

- *Limit disk space to:* Sets the default amount of disk space that users can use

- *Set warning level to:* Sets the default amount of disk space that users can occupy that will trigger a warning message to users that they are reaching their quota

- *Log event when a user exceeds their quota limit:* Causes an event to be entered in the System log to notify the administrator that the user has reached his or her quota

- *Log event when the user exceeds their warning level:* Causes an event to be entered in the System log to notify the administrator that the user is approaching his or her quota

To enable disk quotas, set up default disk quotas and warning levels, prevent users from exceeding their quotas, and receive notification when a user is approaching or has reached his or her quota on a volume (try Hands-on Project 10-4):

1. Open My Computer on the Windows 2000 Server desktop.

2. Right-click the volume on which to set the quotas, and click Properties.

3. Click the Quota tab.

4. Click Enable quota management. (If you later need to eliminate all disk quotas from a particular volume, you can do that by removing the check mark in front of Enable quota management.)

5. Click Deny disk space to users exceeding quota limit.

6. Click the radio button for Limit disk space to, and enter the limitation value, such as 100 MB.

7. Enter values in the Set warning level boxes, such as 90 and MB.

8. Place a check mark in front of Log event when a user exceeds their quota limit.

9. Place a check mark in front of Log event when a user exceeds their warning level.

10. Click OK (see Figure 10-11).

11. If you see a warning that you are about to enable the disk quota system, click OK.
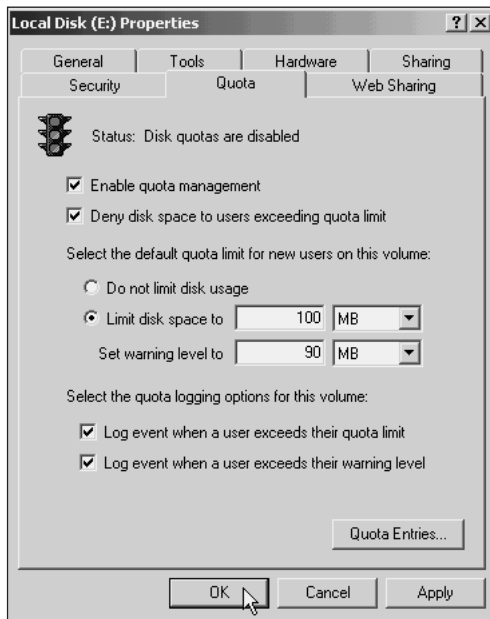
Figure 10-11   Setting default disk quotas

Disk quotas for specific user accounts that are exceptions to the default quotas are set by clicking the Quota Entries button on the dialog box shown in Figure 10-11. For example, to establish a disk quota for the account RKurkowski:

1. Click the Quota Entries button on the Quota tab.

2. Click the Quota menu and click New Quota Entry.

3. Double-click the RKurkowski account (which is listed by the full user name, account name, and domain) in the Select Users dialog box.

4. Click OK.

5. Click the radio button for Limit disk space to, and enter the disk space limitation, such as 200 MB.

6. Enter the value for Set warning level to, such as 150 MB.

7. Click OK (see Figure 10-12).

8. The Quota Entries dialog box is updated to reflect the quota for that account, so that you have an easy way to quickly view quotas on individual accounts and quota exceptions.
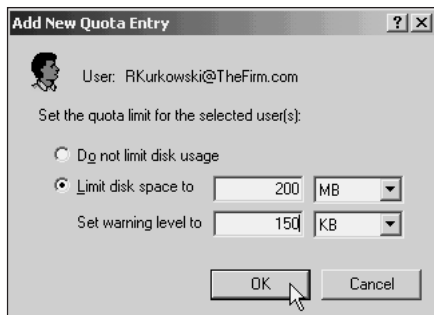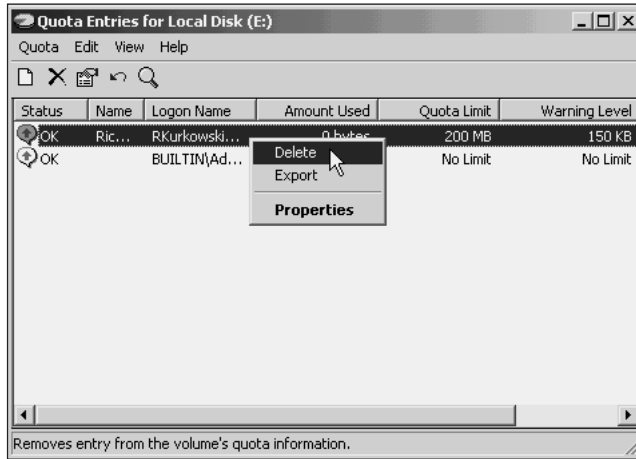

Figure 10-12   Setting a disk quota on a designated user account

The disk quota set on a particular account can be modified by clicking the Quota Entries button to open the Quota Entries dialog box. Double-click the account you want to modify, and then modify the disk quota parameters in the Quota Settings dialog box. To delete a quota associated with an account, right-click the account in the Quota Entries dialog box and click Delete, as in Figure 10-13. The disk quota associated with a particular user can change when ownership of files transfers from one owner to another. For example, consider Rick Kurkowski, who creates the Expenses.mdb database file that occupies 522 KB on a volume that contains a shared folder. After Rick creates Expenses.mdb, his available disk usage is decremented by 522 KB. When Rick's work assignment changes and Jason Brown takes ownership of Expenses.mdb, Rick's available disk usage goes up by 522 KB and Jason's is decremented by the same amount.

> **TIP**   You can view the disk quota limit and warning level set on any account and the amount of disk space used by an account by clicking the Quota Entries button, which opens the information in the Quota Entries dialog box.

Figure 10-13   Deleting a disk quota on an account

When you enable disk quotas, but do not limit disk usage, you have the ability to gather information to plan disk capacity before setting up quotas. An easy way to use the information is to import the statistics on disk usage to a spreadsheet, database, or word-processed file (for example, into a Microsoft Word table). In general, the steps to accomplish this are:

1. Open the preformatted spreadsheet, database, or word-processed file that will hold the information, such as Microsoft Excel.

2. Right-click the volume on which you have collected disk usage information.

3. Click Properties and then click the Quota tab.

4. Click the Quota Entries button.

5. Click the Edit menu and click Select All to select all of the information to copy, or hold down the Ctrl key and click each entry that you want to copy.

6. Drag the information that you have selected into the spreadsheet, database, or word-processed file.

INSTALLING AND MANAGING APPLICATION SOFTWARE

There are several important issues to consider before installing application software for users to access or set up from a server. These include the following:

- Software licensing
- Network compatibility
- Temporary files
- Network performance
- Software testing
- Loading software from the network

Application software is licensed to the user as explained in the software licensing agreement. The server administrator should carefully read and follow the licensing agreement before

loading software. Some companies offer site licensing for unlimited access to the software through the network. Others restrict software licensing to groupings, such as "5-packs" or "10-packs." Some come with license monitoring built into the software, whereas others rely on the server administrator to monitor use, for example by using the Microsoft License Manager or by placing a user access limit on a shared folder. **License monitoring** involves creating a mechanism to ensure that network users do not access software in numbers larger than the software license allows.

Some applications, such as desktop publishing programs, may not be designed to run from a network. In these cases, the best solution is to consult with the vendor about how to adapt the software for a network, if possible. The best advice is to check all applications to be certain they are network compatible. **Network–compatible programs** are designed for multiuser access, often with network capabilities such as options to send files through e-mail.

The network load generated by an application is another issue. Some database applications create high levels of traffic, particularly if the entire database is sent each time a user wishes to examine only a small amount of information. Database reporting tools, graphics, and computer-aided design programs also may generate high traffic. Traffic is not likely to be a problem on a small network, but it is important to closely monitor network activity associated with applications.

Some applications create temporary or backup files while the application is running. For example, Microsoft Word creates backup files so work can be restored after a power failure or computer problem. It is important to determine what extra files are needed to run an application and where to store them. For example, Word backup files can be directed to the user's home folder or to a local folder on the client through Word setup. Plan to teach software users how to deploy temporary and backup files created by software. Also, show users how to delete old temporary and backup files no longer needed.

Plan to test each software installation before releasing it to the users. You might test it from two or more special server accounts created for that purpose. Another way to test software is to first install and test it on a Windows 2000 Professional workstation and then port it to Windows 2000 Server, which is a common technique used by server and network administrators to determine that the software is working and that the permissions are correctly set.

Some applications, such as Microsoft Office, provide the option to install software application files from the network onto each client workstation. Another way is to install client software so application files are loaded from the server each time the application is run. The second way might take a few seconds longer to run the application, because the files are shipped over the network instead of loaded from the user's hard drive. The advantage is a significant savings in disk space on the workstation. A disadvantage is the extra network traffic created on a large network.

Installing Software Using Add/Remove Programs

The best way to install software on a server is to use the Add/Remove Programs icon in the Windows 2000 Server Control Panel. There are two important advantages in using the Add/Remove Programs utility:

- With this method, software configuration is stored in the Windows 2000 Registry. This makes software configuration easier, and configuration information can be updated to the emergency repair disk in case problems develop later.

- The Registry tracks the location of all files associated with software, such as program, initialization, and dynamic-link library (DLL) files. The Registry information makes it easier to remove all program pieces, if necessary.

Consider the installation of Microsoft Office. Before starting the setup, check the licensing information to be sure you have purchased enough licenses for the installation. To install Microsoft Office, insert the Microsoft Office CD-ROM in the server's CD-ROM drive, and then open Add/Remove Programs in the Control Panel. Click Add New Programs and then click CD or Floppy, as shown in Figure 10-14.
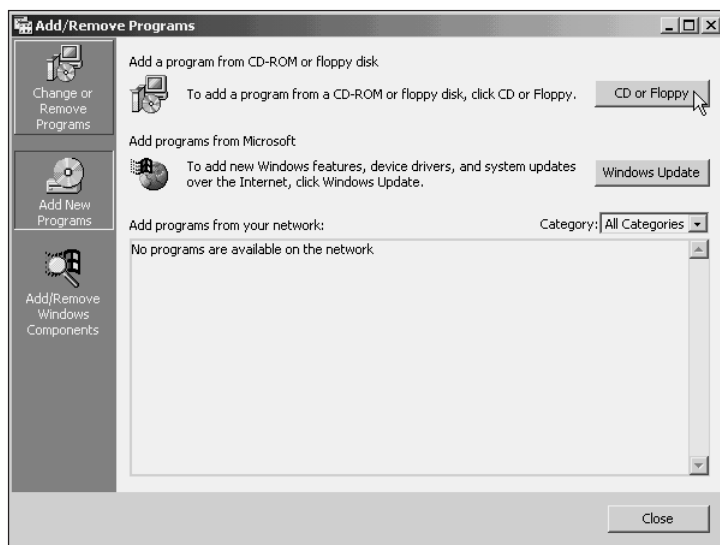
Figure 10-14   Installing application software

The Install Program Wizard takes over with a request to insert the setup disk in the floppy or CD-ROM drive. Click Next and then wait for the wizard to automatically detect the setup file (see Figure 10-15), or click the Browse button to provide the path to the setup file, such as the Microsoft Office setup program on the CD-ROM drive. With the correct path and installation program name entered, click Finish. Now started, the Microsoft Office setup program takes over providing different options to install the Office software. After the software is installed, create a shared folder such as Msoffice, and then create a link to the Dfs root for network users to access.
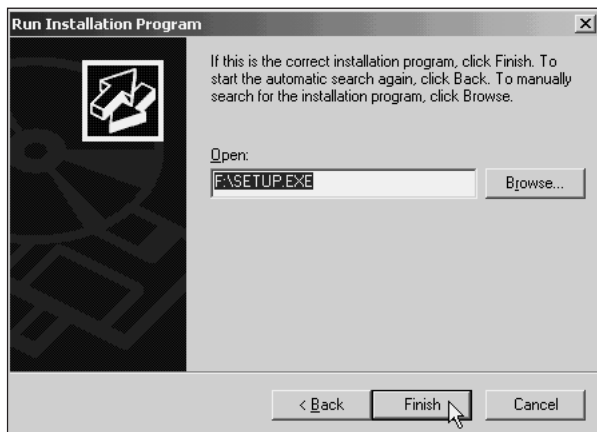
Figure 10-15   Providing the path to the setup program

Running Software Applications in User Mode

When a software application is run on Windows 2000 Server, it runs in **user mode**. This means it does not have direct access to the system kernel, operating system services, CPU, or hardware. Each application runs in its own memory address space, which is the extent to which it affects Windows 2000. The Windows 2000 kernel, consisting of operating system code and services, runs in the privileged **kernel mode**, which also is called the supervisor or protected mode. The operating system programs running in the kernel mode have access to hardware, CPU registers, and I/O functions. They also run in a protected area of memory that cannot be accessed by applications in user mode. If a software application needs to access hardware or an operating system service, it must go through an **application programming interface** (**API**) that serves as a go-between.

The advantage of user mode and kernel mode architecture is that the Windows 2000 operating system is not affected when an application experiences a run-time error or coding bug. Also, the operating system is not affected when a program hangs or has a problem handling memory. The disadvantage is that extensive use of APIs by a program can create system overhead due to the drain on memory and CPU resources.

When you run applications that use graphics, such as the OpenGL graphics screen savers mentioned in Chapter 6, these can put an extra load on a Windows 2000 server because graphics services run in kernel mode instead of user mode. The load is created when an application makes heavy use of the API that communicates between the kernel mode graphics services and the user mode graphics DLLs. Microsoft has developed a way to optimize memory for graphics communications between the kernel and user modes, but you still should watch the impact that graphics programs have on the server (see Chapter 14).

USING THE REGISTRY TO CONFIGURE THE OPERATING SYSTEM SETUP AND SOFTWARE

The Windows 2000 **Registry** is a very complex database containing all information the operating system needs about the entire server. For example, the initialization files used by earlier versions of Windows operating systems, including the critical System.ini and Win.ini files, are contained in the Registry. They also may exist as separate files, but this is only necessary for programs that are not designed for compatibility with the Registry, such as early MS-DOS and pre-Windows 95 programs. Some examples of data contained in the Registry are as follows:

- Information about all hardware components, including the CPU, disk drives, network interface cards, CD-ROM drives, and more
- Information about Windows 2000 services that are installed, which services they depend on, and the order in which they are started
- Data about user profiles and Windows 2000 Server group policies
- Data on the last current and last known setup used to boot the computer
- Configuration information about all software in use
- Software licensing information
- Control Panel parameter configurations

There is the option to use either of two editors to view the contents of the Registry: Regedit or Regedt32. Regedit is an earlier 16-bit version of the Registry editor and is preferred by some administrators because it has the most complete utility to search for keys, subkeys, values, data, and strings. A **key** is a category or division of information within the Registry. A single key may contain one or more lower-level keys called **subkeys**, just as a folder may contain several subfolders. A Registry **value** is a data parameter associated with a software or hardware characteristic under a key (or subkey). A Registry value consists of three parts—a name, the data type, and the configuration parameter—for example, ErrorControl:REG_DWORD:0 (ErrorControl is the name, REG_DWORD is the data type, and 0 is the parameter setting). In this value, the option to track errors is turned off if the parameter is 0, and error tracking is turned on if the value is 1. There are three data formats: DWORD is hexadecimal, string is text data, and binary is two hexadecimal values.

The Regedit editor window is very straightforward, with common menu utilities such as Registry, Edit, View, and Help. Regedt32 is a much fancier 32-bit editor with cascading windows and twice the number of menu bar options as Regedit. It has added options that manage Registry security, that sees information in expanded views, that sets up auditing to track who has accessed the Registry, and added keys or values, and that sets up access to the Registry in read-only mode to ensure against mistakes (try Hands-on Project 10-5 to practice using Regedt32).

10

> **TIP** Neither Registry editor is automatically available from a menu or icon in Windows 2000 Server. Regedit is located in the Winnt folder, and Regedt32 is in the \Winnt\System32 folder. If you use one or both editors frequently, you will likely want to create a shortcut to access them. Otherwise, many administrators start them by using the Run option from the Start button.

The Registry data is stored in a top–down hierarchy with five root keys at the highest level:

- HKEY_LOCAL_MACHINE
- HKEY_CURRENT_USER
- HKEY_USERS
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_CONFIG

A **root key**, also called a **subtree**, is a primary or highest-level category of data contained in the Registry. It might be compared to a main folder, such as the Winnt folder, which is at the root level of folders. All root keys start with HKEY to show they are the highest–level key.

HKEY_LOCAL_MACHINE

Under the HKEY_LOCAL_MACHINE root key is information on every hardware component in the server. This includes information about what drivers are loaded and their version levels, what IRQs (interrupt requests) are used, setup configurations, the BIOS version, and more. Figure 10-16 shows the Registry contents, using the Regedt32 editor to view the HKEY_LOCAL_MACHINE root key information about serial ports.
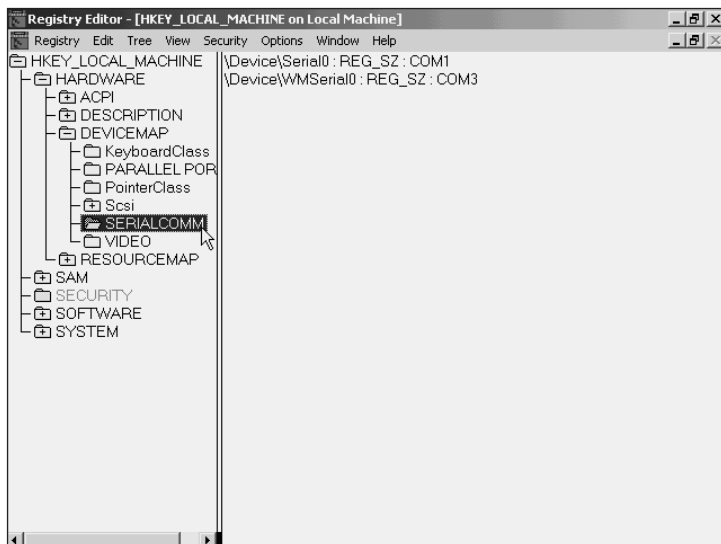

Figure 10-16   The HKEY_LOCAL_MACHINE root key

Under each root key are subkeys, which are HARDWARE, SAM, SECURITY, SOFTWARE, and SYSTEM for the root key in the figure. Each subkey may have subkeys under it, such as ACPI, DESCRIPTION, DEVICEMAP, and RESOURCEMAP under the HARDWARE subkey in Figure 10-16.

A few subkeys are stored as a set, called **hives**, because they hold related information. This is true for the SOFTWARE subkey, which holds information about installed software. You can make hardware configuration changes directly from the Registry, although this is not recommended (see the following Caution). For example, if Windows 2000 Server has incorrectly detected three serial ports, but only two are actually installed, you can delete one by using the Registry editor. For instance, to delete serial port 3, highlight the line in Figure 10-16, \Device\WMSerial0:REG_SZ:COM3, and then press Del, or open the Edit menu and click Delete.

CAUTION

> Although it is possible to make hardware configuration changes directly from the Registry, this is a dangerous undertaking, because a wrong deletion may mean you cannot reboot your server into Windows 2000 Server. It is better to use other options first, such as the Control Panel. Make changes in the Registry only under the guidance of a Microsoft technical note or a Microsoft support person.

10

HKEY_CURRENT_USER

The HKEY_CURRENT_USER key contains information about the desktop setup for the account presently logged on to the server console. It contains data on color combinations, font sizes and type, the keyboard layout, the Taskbar, clock configuration, and nearly any setup action you have made on the desktop. For example, if you want to change the environment parameter governing where temporary files are stored for applications, you can do it from here. The new path is set by clicking the Environment subkey under the HKEY_CURRENT_USER root key and changing the path shown as the value in the right pane. The sounds associated with a given event can be set by clicking the path \HKEY_CURRENT_USER\AppEvents\EventLabels and then changing the sound value for a particular event, such as the event to close a window, which is a single value in the Close subkey (\HKEY_CURRENT_USER\AppEvents\EventLabels\Close).

Another example is to change a program that runs in association with a particular file extension. For example, click the following path: \HKEY_CURRENT_USER\Software \Microsoft\Windows NT\CurrentVersion\Extensions (Figure 10-17; notice there are so many subkeys that not all of the path fits into a single screen display). If the Notepad program is associated with files ending in .txt, you can make a change to have Wordpad start instead. To do this you would change the value, "txt:REG_SZ:notepad.exe ^.txt" to "txt:REG_SZ:write.exe ^.txt," because Write.exe is the file that starts the Wordpad application.
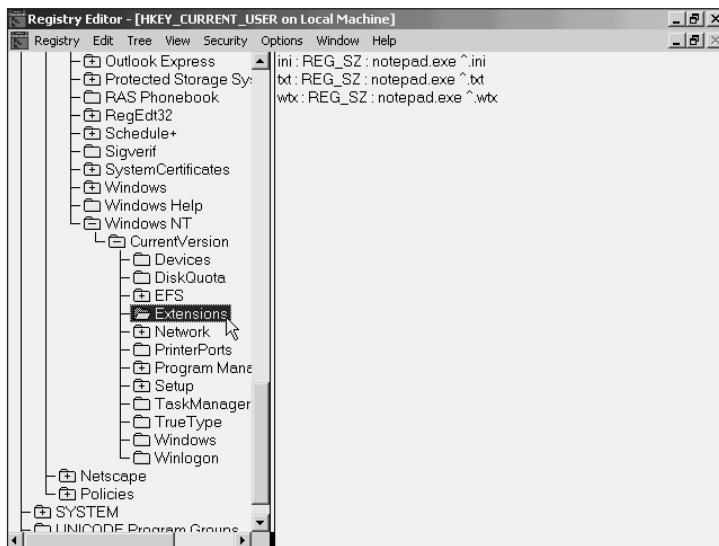
Figure 10-17   Changing Registry data for file associations

HKEY_USERS

The HKEY_USERS root key contains all of the user profiles kept on the server for all users. Each profile is listed under this root key. Within each user profile there is information identical to that viewed within the HKEY_CURRENT_USER root key. The profile used when you are logged on is one of the profiles stored under HKEY_USERS. You can make the same changes just examined, by finding the subkey for your profile and making the changes here instead of under the HKEY_CURRENT_USER root key.

HKEY_CLASSES_ROOT

The HKEY_CLASSES_ROOT key holds data to associate file extensions with programs. This is a more extensive list than the one viewed under HKEY_CURRENT_USER. Associations exist for executable files, text files, graphics files, clipboard files, audio files, and many more. These associations are used as defaults for all users who log on to Windows 2000 Server, whereas the associations in HKEY_CURRENT_USER and HKEY_USER are those that have been customized for a given user profile.

HKEY_CURRENT_CONFIG

The last root key, HKEY_CURRENT_CONFIG, has information about the current hardware profile. It holds information about the monitor type, keyboard, mouse, and other hardware characteristics for the current profile. On most servers, there is only one default hardware profile set up. Two or more profiles could be used, but this is more common for a portable computer running Windows 2000 Professional that is used with and without a docking station. One profile would have the keyboard and monitor used when on the road, and another would have a larger keyboard and monitor used when the computer is docked.

SETTING UP AND USING THE LICENSE MANAGER

Microsoft includes a licensing monitor tool called the License Manager in Windows 2000 Server. The License Manager works for Microsoft products, such as Windows 2000 Server, and for the Microsoft BackOffice products, such as Microsoft Exchange Server for e-mail, Internet Information Services for Internet connectivity, Systems Management Server to help manage network workstations and software, and SQL Server for large databases.

The License Manager is equipped to monitor licensing on a per seat or per server basis (see Chapter 5). Per seat licensing means that there needs to be a license to run a software application for the computer on which that software is loaded, no matter whether the executable files are loaded over the network from the server or from a folder on that workstation's hard disk. If there are 72 computers on a network that need to run a program, such as Microsoft Word, then there must be 72 licenses. The per server licensing approach places the licensing burden on the server instead of on the workstation. In the per server method, there only need to be enough licenses for the maximum number of client workstations that use a software application at a given time. For example, in per-seat licensing, the highest number of people who use Microsoft Word simultaneously might be 22, even though there are 72 total workstations connected to the network. In this case, only 22 Microsoft Word licenses are needed for that server. When you purchase software licenses, make sure you understand what type of licensing you are getting, and set up the license monitoring to match the type of license you have. Costs for per seat licenses are often different from costs for per server licenses. Also, some software vendors license only to a specific computer and have no per seat or per server arrangement, making that software difficult to employ in a network environment. Always read the license information or check with the software vendor to make sure you understand the licensing stipulations.

Besides tracking the per seat and per server license privilege, the License Manager is used to add new licenses or to delete licenses. Also, it can replicate licensing to other Windows 2000 servers in a domain. Thus if you have 1000 licenses for a BackOffice product and 15 Windows 2000 servers, the License Manager can spread the licenses across all servers or workstations (depending on the licensing mode). The License Manager does not stop use of software when the number of users exceeds the number of licenses, it only keeps statistics on use and provides information when there is a need to purchase more licenses. However, it does have the capability to revoke a software license for a user or to limit licensing for a particular server.

The first step in setting up the License Manager is to make sure the License Logging Service is enabled and set to automatically start when the server is booted. The procedure to do that is the same as for configuring the File Replication Service discussed earlier, except that you look for the License Logging Service in the list of services.

The next step is to open the Administrative Tools menu and click Licensing. Click the License menu and then New License. The New Client Access License dialog box opens, as shown in Figure 10-18, from which you can add new licenses as you purchase them (try Hands-on Project 10-6).

10

Figure 10-18   Adding new licenses

To view the software that is installed, click the View menu in the License Manager, and click Products View. The installed products are listed with information about the per-seat and per-server allocation of the licenses, plus the maximum license use that has been reached. Other information is available as well, such as the purchase history. To view the license usage statistics, click the View menu in the License Manager and then click Clients, which shows the licensed and unlicensed usage.

CHAPTER SUMMARY

❒ Using the Distributed File System (Dfs) enables both you and your users to be more productive. For users, Dfs means that they can more easily find and access important shared folders. For you, Dfs simplifies the management of shared folders, particularly when you manage multiple servers. Dfs can be implemented using the standalone or domain model. When Dfs is implemented in a domain, it can be used to provide fault tolerance, load balancing, and a single place from which to back up critical files.

❒ Disk quotas are an important feature for any type of server, whether standalone or in a domain. Before disk quotas, it was possible for the rapid accumulation of files, particularly temporary and unused files, to occupy huge amounts of disk space. By enabling disk quotas, you can accomplish two important tasks: (1) obtain statistics for disk capacity planning and (2) place limits on the amount of disk space that individual users can occupy. Disk quotas can be used in a positive sense to help users learn how to clean up unused files, make more disk space available for all purposes, and save money on disk resources.

❒ The Add/Remove Programs tool in the Control Panel is provided to help you manage software installations, easily upgrade software, and easily remove software. Add/Remove Programs works with the Registry to configure software and track software elements. When you install software, there may be times when it is necessary to edit the Registry as a way to tune a particular software or hardware feature.

❒ When you install software, plan to use the Microsoft License Manager to help track the available licenses and determine when more licenses must be purchased.

The next chapter focuses on managing local and network printing resources in Windows 2000 Server. Network printing services are yet another resource that is especially popular among users.

KEY TERMS

application program interface (**API**) — Functions or programming features in a system that programmers can use for network links, links to messaging services, or interfaces to other systems.

cache timeout — The amount of time that a Dfs shared folder is retained in the client operating system's cache for fast access.

Dfs link — A path that is established between a shared folder in a domain and a Dfs root.

Dfs root — The main Active Directory container that holds Dfs links to shared folders in a domain.

Dfs topology — Applies to a domain-based Dfs model and encompasses the Dfs root, Dfs links to the root, and servers on which the Dfs structure is replicated.

disk quota — Allocating a specific amount of disk space to a user or application, with the ability to ensure that the user or application cannot use more disk space than is specified in the allocation.

Distributed File System (**Dfs**) — A system that enables folders shared from multiple computers to appear as though they exist in one centralized hierarchy of folders instead of on many different computers.

hive — A set of related Registry keys and subkeys stored as a file.

kernel mode — Protected environment in which the Windows 2000 operating system kernel runs, consisting of a protected memory area and privileges to directly execute system services, access the CPU, run I/O operations, and conduct other basic operating system functions.

key — A category of information contained in the Windows 2000 Registry, such as hardware or software.

license monitoring — A process used on network servers to be certain the number of software licenses in use does not exceed the number for which the network is authorized.

load balancing — On a single server, distributing resources across multiple server disk drives and paths for better server response; on multiple network servers, distributing resources across two or more servers for better server and network performance.

master folder — The main folder that provides master files and folders for a Dfs root or link when replication is enabled.

network–compatible program — Software that can operate in a multiuser environment using network or e-mail communication APIs.

Registry — A database used to store information about the configuration, program setup, devices, drivers, and other data important to the setup of a computer running Windows 2000, Windows NT, Windows 98, or Windows 95.

replica set — A grouping of shared folders in a Dfs root that are replicated or copied to all servers that participate in Dfs replication. When changes are made to Dfs shared folders, all of the participating servers are automatically or manually synchronized so that they have the same copy.

root key — Also called a subtree, the highest category of data contained in the Registry. There are five root keys.

subkey — A key within a Registry key, similar to a subfolder under a folder.

10

subtree — Same as root key.

user mode — A special operating mode in Windows 2000 used for running programs in a memory area kept separate from that used by the kernel and in which the program cannot access the kernel or operating system services except through an API.

value — A data parameter in the Registry stored as a value in decimal, binary, or text format.

REVIEW QUESTIONS

1. The computer planning committee at your company is working to project Windows 2000 Server disk capacity needs for the next two years, as part of the computer equipment budgeting process. Because you are part of the committee, they ask you if there is any way to gather statistics on present disk use over a three-month period to help in making projections. How can you obtain the statistics that they want?

   a. Turn on disk auditing for each user's account, and compile the audit reports.

   b. Set default disk quotas to a low number, and gather statistics based on the resulting reports that users are out of disk space.

   c. Enable disk quotas, and after three months copy the disk quota statistics into a spreadsheet.

   d. There is no easy way to gather the statistics except to ask all employees to calculate the space they use.

2. Which of the following are Dfs models that you can set up in Windows 2000 Server?

   a. standalone

   b. transitive

   c. domain–based

   d. all of the above

   e. only a and b

   f. only a and c

3. You have set up Dfs replication among four servers, but none of the shared folders is being replicated automatically. What might you do to solve the problem?

   a. Make sure that the Dfs replicate permission box is checked for Allow in the Dfs root.

   b. Make sure that you have set up automatic replication and not manual replication.

   c. Use the Computer Management tool to determine if the File Replication service is started.

   d. All of the above may be a source of the problem.

   e. Only a and b are possibilities.

   f. Only b and c are possibilities.

4. You need to uninstall a display monitor driver in Windows 2000 Server so that you can set up a new monitor and driver. Which is the safest way to uninstall the driver?

    a. Use the Device Manager.

    b. Use Regedit to delete the driver in the Registry's HKEY_LOCAL_MACHINE root key.

    c. Use Regdt32 to delete the driver in the Registry's HKEY_LOCAL_MACHINE root key.

    d. Use the Add/Remove Programs icon in the Control Panel.

5. Your assistant is attempting to set up a second Dfs root on a server, but the New Dfs Root Wizard will not let him proceed. What is the problem?

    a. He did not reboot the server after creating the first Dfs root.

    b. The first Dfs root must contain at least two Dfs links before a second Dfs root can be set up.

    c. He did not rescan the disks after creating the first Dfs root.

    d. Only one Dfs root can be created on a server.

6. It is the end of the fiscal year, and your boss has money still budgeted to purchase additional licenses for users to access your Windows 2000 server. Unfortunately, he has waited until the last minute and needs the information by this afternoon. How can you quickly assess present use of licenses?

    a. Check the Server service properties, which can show the number of times users have been prevented from logging on as a result of a shortage of licenses.

    b. Check the statistics in the License Manager.

    c. Check the connection statistics available through the Network and Dial-up Connections tool.

    d. There is no way to gather the information on short notice because you must first set up license quotas on each volume.

7. You currently have shared folders set up on seven Windows 2000 servers, which are in different locations and on different subnets of your organization. Network traffic on two of those subnets is very intense each afternoon. What can you do to balance the load?

    a. Move all of the shared folders to the server on the subnet with the least traffic.

    b. Decrease the cache timeout for each shared folder.

    c. Set up all of the folders via Dfs and use replication.

    d. Set up all of the folders via Dfs and then set the speed of the Dfs links to 100 Mbps for those on the traffic-intense subnets.

10

8. Which of the following is (are) true about permissions used on a Dfs root?

   a. There is no Full Control permission, because only the server Administrator can have the equivalent access.

   b. Special permissions can be set up to customize access.

   c. Dfs permissions must be set up for each Dfs link.

   d. All of the above are true.

   e. Only a and b are true.

   f. Only a and c are true.

9. The chief financial officer of your organization is very opposed to your accessing Microsoft Excel and other application programs on the same server that has the organization's accounting and payroll files, because she believes that if Excel hangs it will make the server inaccessible when she is in the middle of updating a file. What might you say to alleviate her worries?

   a. Explain that application software like Excel runs in user mode.

   b. Explain that application software like Excel runs in kernel mode.

   c. Agree to manually allocate a separate RAM location for the applications that you run.

   d. Set your own disk quota to *Deny disk space to users exceeding quota limit*, so that if you go over your quota it will not affect anyone else's server access.

10. Which of the following can contain hives?

    a. a Dfs link

    b. the Registry

    c. a Dfs root

    d. software licensing groups

11. The management in your organization wants to limit all employees to 7 MB of disk space, on each volume which they can use to store files in shared folders and in home folders. What is the best way to accomplish this?

    a. Set up a default disk quota of 7 MB on each shared volume.

    b. Set up a disk quota for each user via the Active Directory Users and Computers tool.

    c. Set up a disk quota of 7 MB for each user account on each volume.

    d. It is not possible to set up disk quotas of 7 MB, because quotas are set in 2 MB increments.

12. Which of the following are part of the Dfs topology when Dfs is set up in a domain?

    a. roots

    b. replica sets

    c. links

    d. all of the above

e. only a and b

f. only a and c

13. It is better to implement Dfs folder sharing on:

   a. FAT-formatted disks because it is faster using FAT

   b. a domain controller instead of a member server because DNS servers give domain controllers higher priority

   c. NTFS-formatted disks because of better security

   d. standalone servers, which enable a deeper folder/subfolder tree structure

14. Sara and Richard each have a disk quota of 2 MB. Recently Sara has taken ownership of an 800 KB database file previously owned by Richard. How does this action affect their disk quotas?

   a. When ownership of a file is transferred, that file is exempt from the disk quota allotment.

   b. The disk quotas of Sara and Richard are unchanged.

   c. Sara's disk quota is now 2.8 MB, but Richard's stays the same.

   d. Sara has 800 KB less space out of the 2 MB quota, and Richard has 800 KB more.

15. ErrorControl:REG_DWORD:0 is an example of:

   a. a Dfs root

   b. a Registry key

   c. a Registry value

   d. a Dfs script command

16. You set up the Dfs root so that the domain local Users group is allowed Read permissions only. The Docs shared folder that is part of the Dfs setup allows the same group Modify permissions. What permissions does the Users group have for that folder within Dfs?

   a. Read

   b. no permissions, because there is a permission conflict

   c. Modify

   d. Full Control, but without the ability to take ownership

17. You have installed a 32-bit Windows application in Windows 2000 Server that includes many .dll and other files, some of which have been copied to the \Winnt\System32 folder. Today you need to remove that application. How do you remove it?

   a. Delete the desktop icon that starts the application.

   b. Delete the folder that contains the application, and use My Computer to search for its related .dll files and delete those as well.

   c. Delete the .exe file that starts the application.

   d. Use the Add/Remove Programs tool in the Control Panel.

10

18. You have received from an Internet newsgroup a technical alert advising you to change a Registry parameter in all user profiles in Windows 2000 Server. What are you likely to edit in the Registry?

    a. the HKEY_USERS root key

    b. the SYSTEM subkey

    c. the HKEY_CLASSES_ROOT root key

    d. the SOFTWARE subkey

19. Which of the following can be set up in the Dfs root properties?

    a. auditing

    b. taking ownership

    c. permissions

    d. all of the above

    e. only a and c

    f. only b and c

20. How can you delete a Dfs link?

    a. Right-click the link in the Distributed File System management tool, and click Remove Dfs link.

    b. Deactivate the Dfs link and then delete it in the Distributed File System management tool.

    c. Delete its root and then delete the link in the Distributed File System management tool.

    d. To ensure data security, you cannot delete a link after it is created.

21. It is 3:00 p.m. on a Friday afternoon, and several people are calling in a panic to report that they do not see several shared folders on the main server, which you know is home to their Dfs root. What is the first step that you should take?

    a. Restart the File Replication service.

    b. Run to the machine room and make sure that the main server is booted and working normally.

    c. Use the Distributed File System management tool to check the status of the root and of the links in question.

    d. Use the Dfs tool to restart the Dfs root and to rescan its links.

22. Which of the following are maintenance tasks that you can perform on your Dfs system of shared folders?

    a. Regularly check for folders that are no longer in use and that should be deleted.

    b. Periodically check the cache timeout values to make sure that they are appropriate to how particular folders are used.

   c. Use My Computer to periodically move folders from high-impact servers to those with a lower impact, and then establish new links.

   d. all of the above

   e. only a and b

   f. only a and c

23. The lead research scientist in your company needs to work over the weekend to prepare information for a lecture she is presenting on Monday. She does not know how close she is to reaching her disk quota and is calling you to find out. How can you determine where she stands?

   a. There is no way to determine where she stands, but you can increase her quota to make sure there is no problem.

   b. Check the Quota Entries dialog box in the properties of the shared disk volume that she uses.

   c. Open the Command Prompt window and use the Quota command along with her account name to find out.

   d. Use the Distributed File System management tool to query quotas.

24. Your boss has been reading about companies that are lax in making sure that they have enough licenses for the software that they use. You already know that you have enough Windows 2000 Server licenses, but you are not sure about licenses for SQL Server and Exchange Server. How can you find out if use has exceeded the number of licenses for these products?

   a. Check in the License Manager.

   b. Check the Registry, which can track the number of times the license limit has been exceeded.

   c. Look for license alerts displayed by the Registry at the server's console.

   d. Create a license monitor filter to capture the names of accounts that exceed license limitations.

25. Which of the following would you find in the Registry?

   a. keys

   b. subtrees

   c. root keys

   d. all of the above

   e. only a and b

   f. only a and c

10

HANDS-ON PROJECTS

Project 10-1

Suppose that the financial auditors are visiting your organization and you have decided to organize Dfs shared folders for all spreadsheets that they must view. In this project you practice creating a Dfs root using the domain-based model. The server on which you create the root must have no other Dfs root, and the Active Directory must already be installed. Also, before you start, check with your instructor about which drive path to use for the Dfs root.

To create a Dfs root:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Distributed File System**.
2. Click **Distributed File System** in the console tree.
3. Click the **Action** menu, click **New Dfs root**, and click **Next** after the New Dfs Root Wizard starts.
4. Click **Create a domain Dfs root**, if it is not already selected. Click **Next**.
5. Make sure the domain name is displayed in the Domain name box, or use a different domain per your instructor's permission. What other information is displayed in the dialog box? Click **Next**.
6. Click the **Browse** button to find the server. What information is displayed in the Find Computers window that can help you locate a server, such as a domain controller? Double-click the server on which the Dfs root will reside, and then click **Next**.
7. Click **Create a new share**. Enter the path specified by your instructor, such as **D:\Spreadsheets**, and enter **Spreadsheets** as the share name. Click **Next**. Click **Yes** to confirm that you want to create a new folder.
8. Use the default Dfs root name, **Spreadsheets**, and enter the comment **Sales history spreadsheets**. Click **Next**.
9. Examine the summary of information that you specified. How might you reenter information if you find that you made a mistake in earlier steps? Record the summary information in your lab journal or in a word-processed document. Click **Finish**.
10. Look for the new root in the console tree under Distributed file system.
11. Leave the console tree open for the next project.

Project 10-2

In this project, you practice creating, customizing, and then deleting a Dfs link in preparation for the auditors. Before you start, obtain the name and location of a shared folder from your instructor (or create a shared folder on the server from which you are working, and use that folder for this project).

To create the new Dfs link:

1. Right-click the **Spreadsheets** root under the tree in the left pane.
2. Click **New Dfs Link**.

3. Enter **Projects** in the Link name box. What happens in the *When a user opens* text box as you enter the link name? Click **Browse** to find the computer and shared folder that you obtained from your instructor (or that you created in advance for this project). Provide a comment to describe the link, such as **Project costs**.

4. Enter **2000** in the Clients cache this referral for _____ seconds box.

5. Click **OK**. (If you get an error message, make sure that the account you are using has access to the shared folder for the link, that you have a good network connection, and that the computer with the shared folder is compatible with Dfs.)

6. In the left pane, click the link you created, if it is not already highlighted. What information is displayed under the Replica(s) column in the right pane? Record your observations in your lab journal or in a word-processed document.

Assume that the contents of the link you created will not change often and that you need to customize the cache timeout.

To customize the cache timeout for a Dfs link:

1. Right-click the link you created, and click **Properties**.

2. Make sure the **General** tab is displayed.

3. Notice the value already set in the Clients cache this referral for _____ seconds parameter and record your observation in your lab journal or in a word-processed document.

4. Enter **500** as the new cache timeout value.

5. Click **OK**.

When the auditors are finished with this particular link, you delete it in an effort to keep unneeded links from proliferating.

To remove the Dfs link that you just created:

1. Right-click the link that you created in the left pane.

2. Click **Remove Dfs Link**.

3. Click **Yes**.

4. Note in your lab journal or in a word-processed document if there is a way to recover the link, such as from the Recycle Bin or by clicking an Undo button.

Project 10-3

In this hands-on activity assume that the financial auditors in your organization will need to access the Dfs root link, but your boss wants you to make sure they cannot write to any of the folders. Finally, you will delete the Dfs root that you created in Project 10-1, after the auditors are finished examining the information.

To set up security:

1. Right-click the **Spreadsheets** root that you created in Project 10-1.

2. Record the options that you see in your lab journal or in a word-processed document.

3. Click **Properties**.

4. What tabs are displayed in the Properties dialog box? What is the purpose of each tab?

5. Click the **Security** tab.

6. How do the options on this tab compare with those that you would find on a regular Windows 2000 Server folder? What groups are already assigned permissions for the Dfs root?

7. Click **Authenticated Users** and notice what permissions this group has.

8. Click the **Add** button.

9. Double-click the **Guests** group (or another group that is not already listed in Step 6), and click **OK**.

10. What permissions are automatically given to the Guests group (or other group that you used in Step 9)?

11. Click the **Deny** box for the **Write** permission. Click **Apply** and then click **Yes**.

12. Practice removing the Guests group by clicking that group and then clicking **Remove**. Click **OK**.

To delete the Dfs root:

1. Right-click the **Spreadsheets** root that you created in Project 10-1.

2. Click **Delete Dfs Root**.

3. Click **Yes** to confirm the deletion.

4. Close the Distributed File System console.

Project 10-4

The main disk on your server contains user home folders, and you discover that users are rapidly occupying vital disk space. In this project you set up default disk quotas on that NTFS volume.

To configure the default disk quotas:

1. Open **My Computer** and right-click an NTFS formatted volume, such as drive **C**.

2. Click **Properties** and then click the **Quota** tab. If the Quota tab is not displayed, what does this mean?

3. Click **Enable quota management** if it is not already selected.

4. Click **Deny disk space to users exceeding quota limit** if it is not already selected.

5. Click **Limit disk space to** and enter **20** in the first box, then select **MB** in the box next to it.

6. Enter **18** and **MB** as the warning level.

7. Click **Log event when a user exceeds their quota limit**.

8. Leave the box blank for **Log event when a user exceeds their warning level** (to reduce the number of event log entries).

9. Click the **Quota Entries** button to view quota entries. How would you set 2 MB as the disk quota limit for the Guest account?

10. Close the Quota Entries dialog box, and then click **OK**. Click **Yes** if you are asked to enable the quota system.

Project 10-5

In this project you view where Control Panel settings are stored in the Registry and practice using the Regedt32 editor.

To view the Control Panel settings:

1. Click **Start**, click **Run**, and enter **regedt32** in the Open box. Click **OK**.

2. Click the **Options** menu and place a checkmark in front of **Read Only Mode** to make sure that you cannot inadvertently change the Registry contents during this project.

3. Access the **HKEY_CURRENT_USER** window and double-click **Control Panel**.

4. What Control Panel subkeys do you see? Record your observations in your lab journal or in a word-processed document.

5. Double-click **Accessibility**. What are the subkeys displayed?

6. Click **MouseKeys** to view the values set for that subkey.

7. Click two or three other subkeys to view their values.

8. Click a value and then click the **Edit** menu to view how to modify a value, delete a value, or add a new one (but absolutely do not make any changes).

9. Close the Registry editor.

Project 10-6

In this activity you view which products are installed via the License Manager, and then you add 10 new Windows 2000 Server licenses that your organization has purchased.

To use the License Manager:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Licensing**.

2. Click the **View** menu and then click **Products View**.

3. Notice the products that are installed under the Product column. Also notice the number of licenses. The last column, Per Server Reached, shows the maximum number of users who have used the licenses at a given time. Record your observations.

4. Click **Windows Server** under the Product column.

5. Click the **License** menu and then click **New License**.

6. Make sure **Windows Server** is selected in the Product scroll box.

7. Enter **10** in the Quantity box.

8. Click the radio button for the License mode, Per Seat or Per Server (unless this is already selected by default).

10

9. Add the comment **New licenses for student lab**.

10. Click **OK**. If a licensing agreement message is displayed, check the box to indicate that you agree with the licensing terms and then click **OK**. Close the License Manager.

CASE PROJECT

Aspen Consulting Project: Configuring Dfs, Disk Quotas, and Licensing

Precision Digital is a company that makes compact discs for digital use, such as CD-ROMs, CD-Rs, and CD-RWs. They design, manufacture, sell, and research discs entirely for computer-related digital applications. Precision Digital has employees located in four buildings, and there is a Windows 2000 server in each building. All servers are in one domain. One building houses the administrative and business offices, one is used for research teams, and the other two are used to manufacture discs. Precision Digital's server administrator has just resigned, and they are in the process of hiring a new one. In the interim, they have hired you through Aspen Consulting to help work on several special projects.

1. Each server contains from 10 to 20 shared folders that are accessed by various users throughout the company. The problem is that users are still very confused about which folders are on which servers. As a result, they waste a lot of time trying to find the information that they need. Precision Digital asks you to help them develop a way to make the folders easier to find and access. Explain to Precision Digital's administrative team how Dfs works and how it can be of value in their situation. Suggest a very general Dfs folder structure that they might implement.

2. After you make your presentation about Dfs, the human resources director at Precision Digital calls to let you know that they have hired a new server administrator, but the new administrator has only worked with other server operating systems, not with Windows 2000. Prepare an explanation for the new administrator about how to set up Dfs in a domain.

3. While you are training the new administrator, you receive a call from a research team leader that one of the volumes on the server used by the research groups is full. Your first recommendation is to have users delete old and temporary files on that volume. The team leader mentions that none of the company's servers is set up to limit the amount of disk space that a user might occupy. Discuss how the company can set limits on disk usage and how it can better plan disk capacity in the future.

4. One of your projects is to install Microsoft Office on the server used by the administrative offices. Explain in general terms how to install the software. Also, prepare a checklist for the new administrator about the steps to take before installing new software on a server.

5. The previous administrator purchased 20 new licenses for the administrative server. Explain how to install the licenses. Also, explain how to view the current license usage statistics.

OPTIONAL CASE PROJECTS FOR TEAMS

Team Case One

Because Dfs can be of vital importance to organizations, Mark Arnez is concerned about developing a table with steps or a flowchart for troubleshooting Dfs. He asks you to form a group to develop a complete set of troubleshooting steps.

Team Case Two

Setting disk quotas has two dimensions: political and technical. Mark Arnez asks you to form a group to explore both elements for setting up disk quotas. Create a report in which the first section deals with how to prepare users in an organization for the implementation of disk quotas. In the second section, explain different scenarios for setting up disk quotas, such as scenarios involving default quotas, individual user account quotas, and gathering information about disk use before setting quotas.

10